



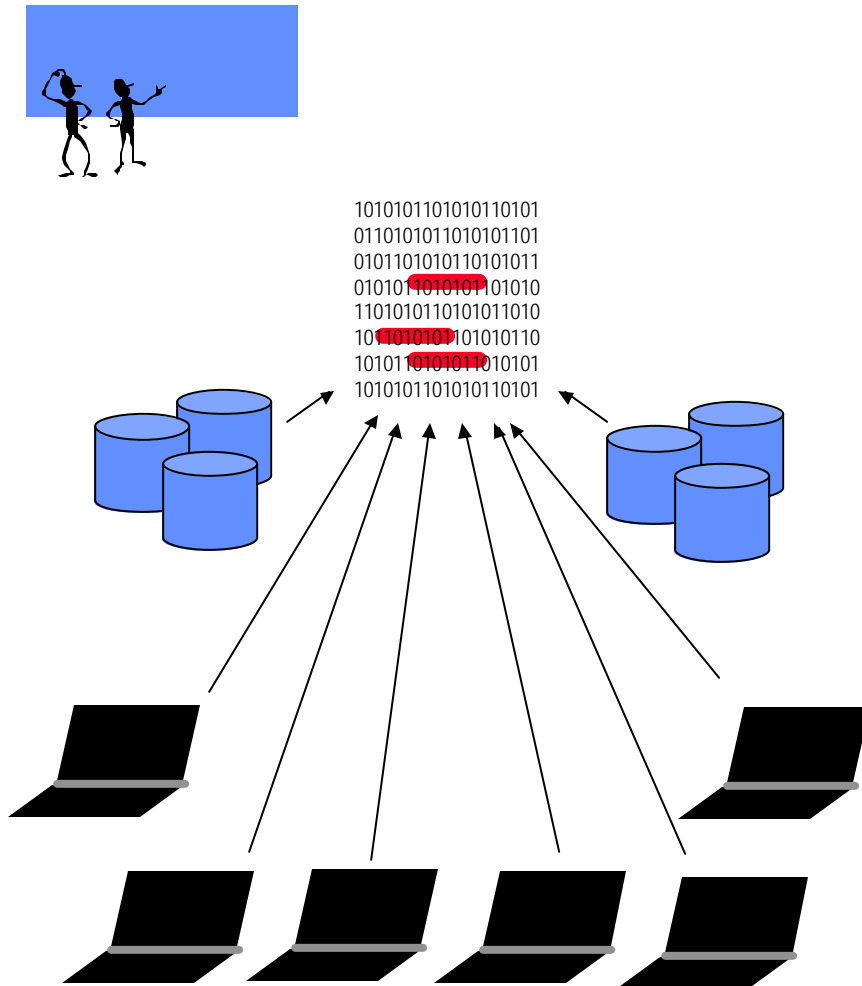
Defense Advanced Research Projects Agency
Information Assurance and Survivability
Operational Experimentation
(OPX)

Phoenix Challenge 2002

Brian Witten
OPX Program Manager
bwitten@darpa.mil

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.				
1. REPORT DATE (DD-MM-YYYY) 22-04-2002		2. REPORT TYPE Briefing		3. DATES COVERED (FROM - TO) xx-xx-2002 to xx-xx-2002
4. TITLE AND SUBTITLE Information Assurance and Survivability Operational Experimentation (OPX) Unclassified			5a. CONTRACT NUMBER	
			5b. GRANT NUMBER	
			5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Witten, Brian ;			5d. PROJECT NUMBER	
			5e. TASK NUMBER	
			5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME AND ADDRESS DARPA XXXXX, XXXXXXX			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS DARPA ,			10. SPONSOR/MONITOR'S ACRONYM(S)	
			11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT APUBLIC RELEASE ,				
13. SUPPLEMENTARY NOTES				
14. ABSTRACT See report.				
15. SUBJECT TERMS IATAC Collection				
16. SECURITY CLASSIFICATION OF:		17. LIMITATION OF ABSTRACT Public Release	18. NUMBER OF PAGES 17	19. NAME OF RESPONSIBLE PERSON email from Booz, Allen & Hamilton (IATAC), (blank) lfenster@dtic.mil
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified	19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007	
				Standard Form 298 (Rev. 8-98) Prescribed by ANSI Std Z39.18

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 074-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE 4/22/2002	3. REPORT TYPE AND DATES COVERED Briefing 4/22/2002	
4. TITLE AND SUBTITLE Information Assurance and Survivability Operational Experimentation (OPX)			5. FUNDING NUMBERS	
6. AUTHOR(S) Witten, Brian				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) DARPA			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Advanced Projects Research Agency			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; Distribution unlimited			12b. DISTRIBUTION CODE A	
13. ABSTRACT (Maximum 200 Words) This briefing was presented during the Phoenix Challenge 2002 Conference and Warfighter Day.				
14. SUBJECT TERMS IATAC Collection, information assurance			15. NUMBER OF PAGES 16	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UNLIMITED	



- New Capability:
Situational Awareness
- Reduce Overload:
Analyst Workbench
- Protect Centers of Gravity:
Survivable Servers
- Pervasive Sensors:
Hardened Clients

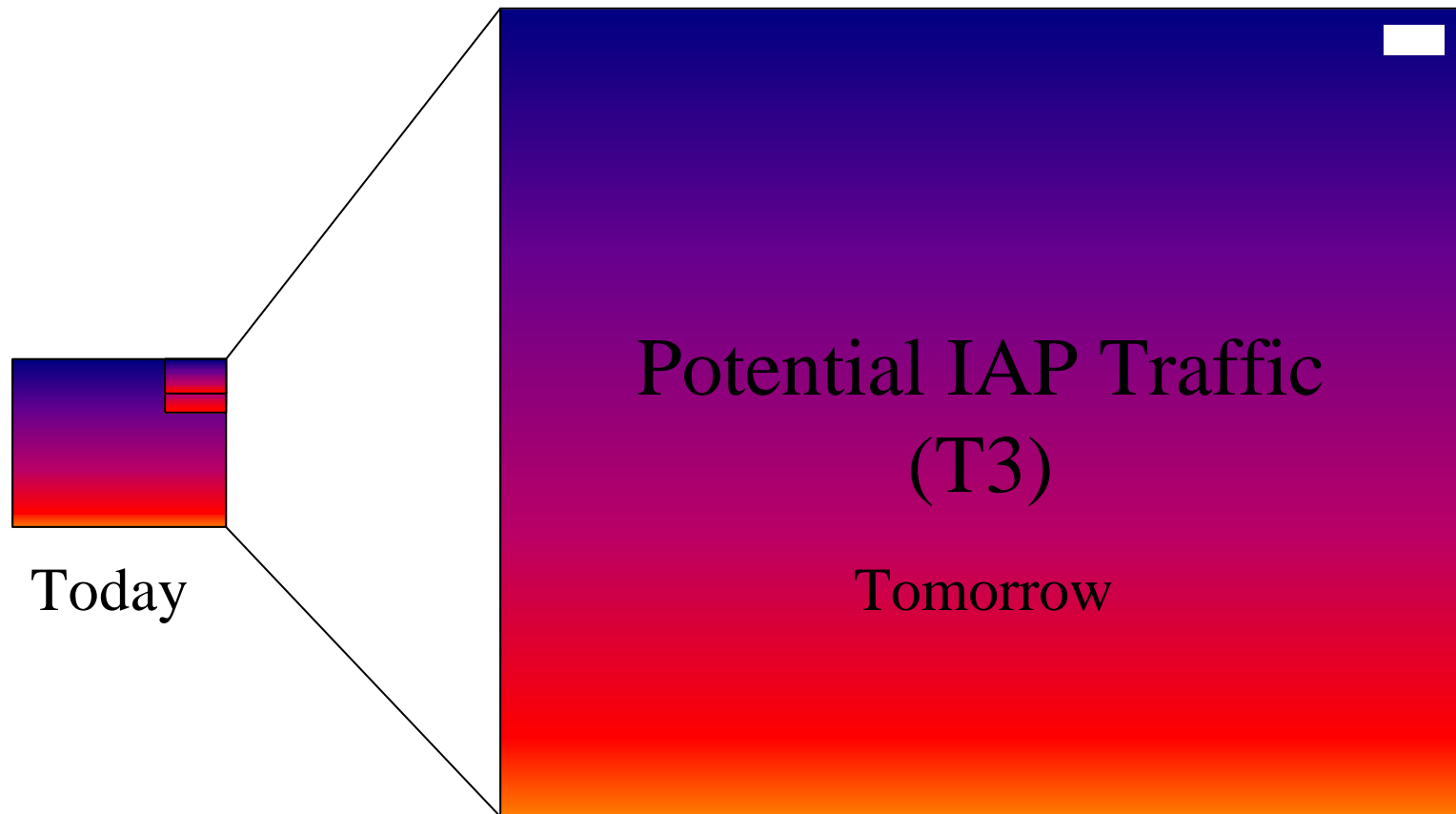


Strategy



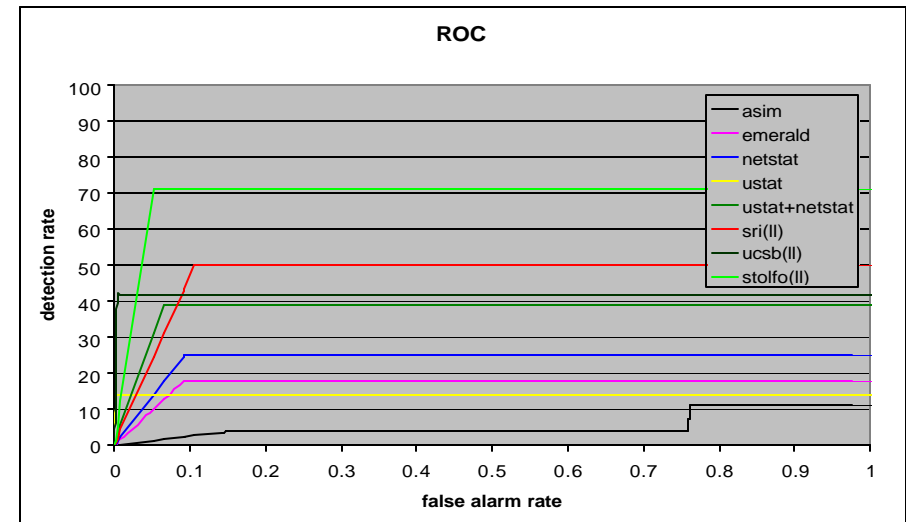
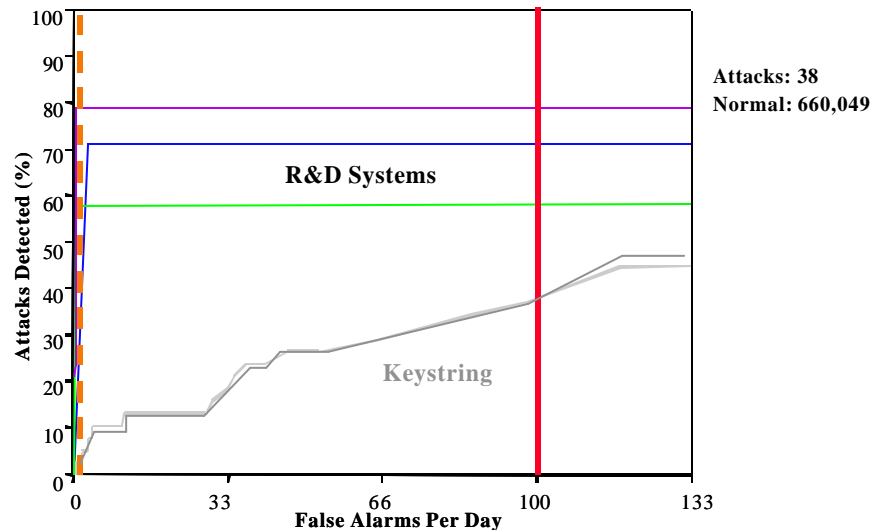
- **Objectives:**
 - ◆ Accelerate transition of effective technologies
 - ◆ Inform research agenda with operational experience
- **Key Experimentation Risks, Transition Metrics:**
 - ◆ Limited operational staff time
 - ◆ Impact on operational systems
- **Approach:**
 - ◆ Leverage mature research, well tested in lab
 - ◆ Field cautiously: walk before we run

Impact of Transition to T3 volume at Internet Access Points





Intrusion Detection in the Lab



DARPA 1998 Results (MIT/LL and AFRL)

- Operational sensors:
 - ◆ Hundreds of false alarms per attack
 - ◆ Actually miss most attacks
- Research sensors:
 - ◆ Dramatically reduce false alarm rates
 - ◆ Substantially improve detection coverage



Analyst Workbench



-
- Analysts currently overwhelmed
 - ◆ Flood of data, high false alarm, low detection rates
 - ◆ Not... real time, decision quality, always actionable
 - DARPA Algorithms
 - ◆ Over a dozen lab tested real time algorithms
 - ◆ Data mining, anomaly, self organizing, expert systems
 - Execution: September 2001 – September 2002

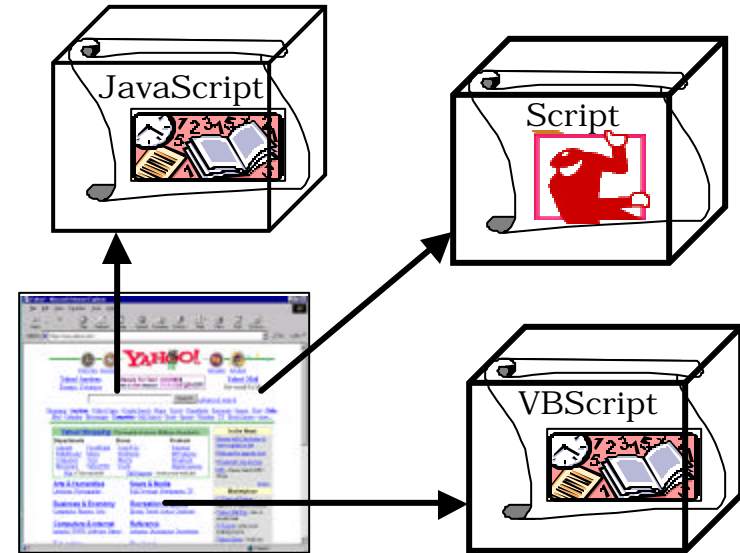
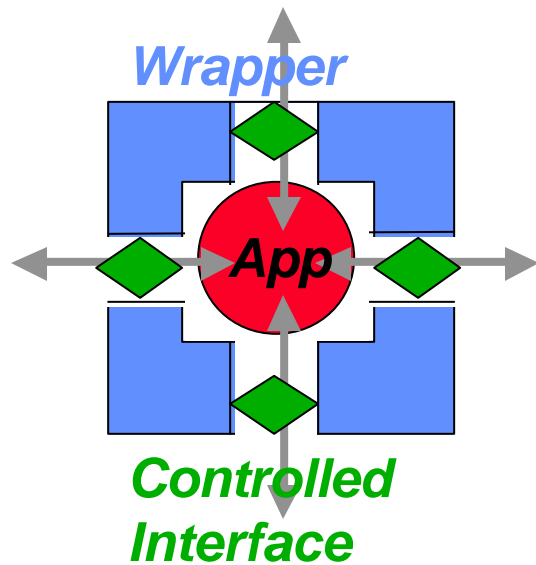


Hardened Client

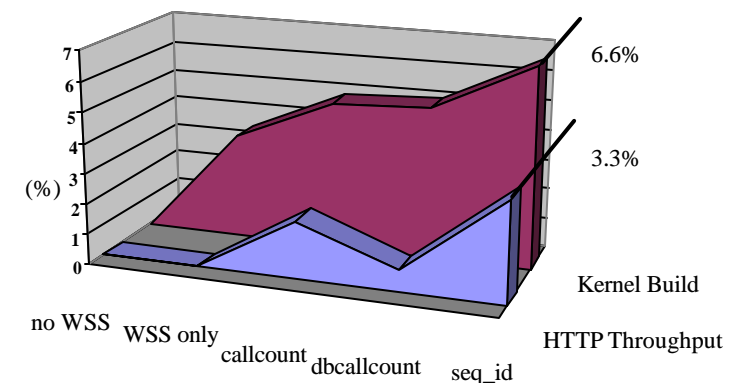


-
- **MARFORPAC Challenge**
 - ◆ Classic SIPR/NIPR PC problem
 - ◆ Compounded by TAD laptop theft
 - ◆ Insider threat and unknown viruses

 - **Proposed Technology**
 - ◆ Safe e-mail “wrappers” and encrypting file system
 - ◆ Autonomic Distributed Firewall
 - ◆ PGP Disk & Disk Eraser



- Trap and stop unknown viruses
- Enable safer use of mobile code
- Performance impact: Low
- Availability: Solaris, Linux, NT, Win2K

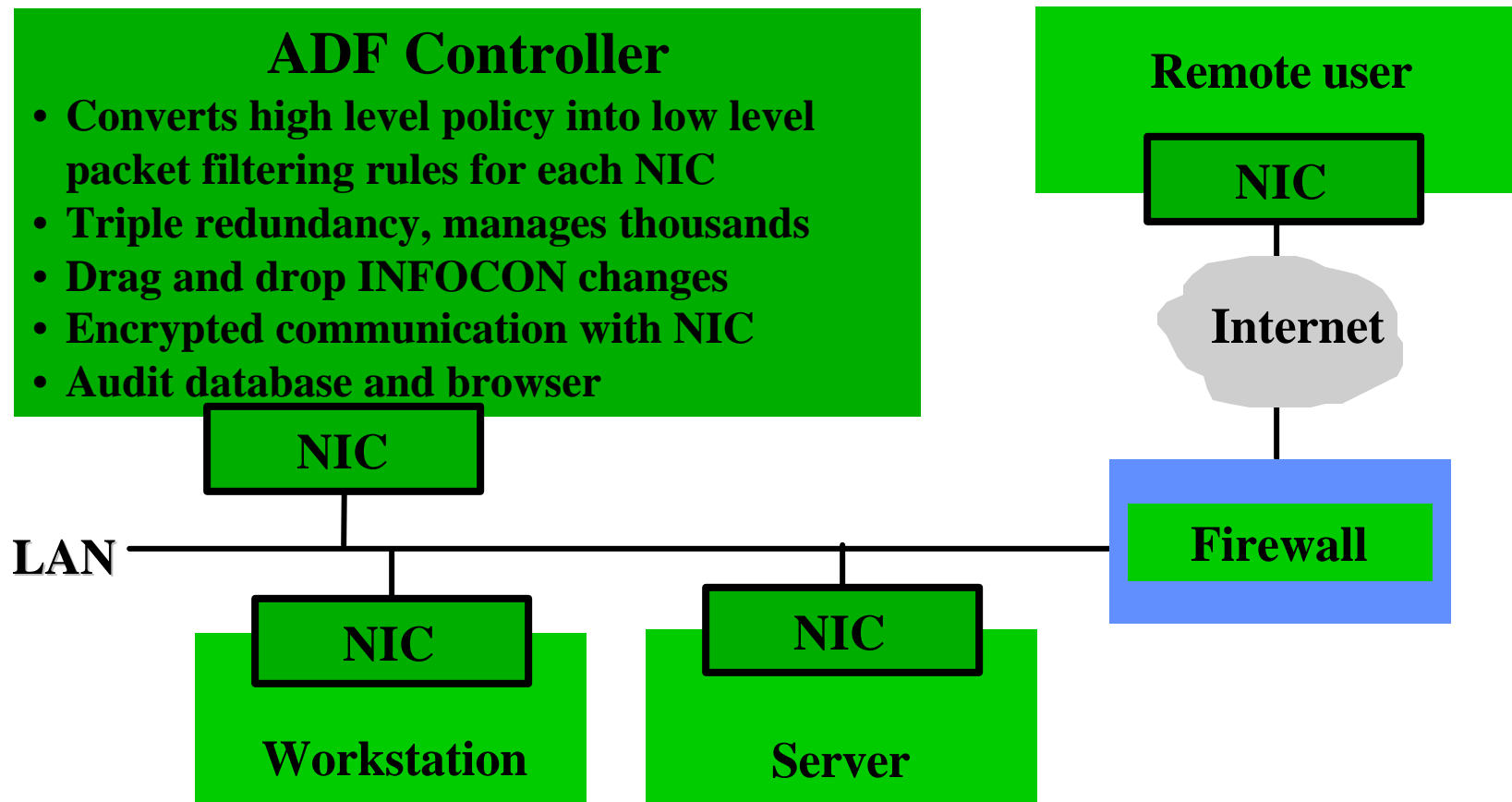




Autonomic Distributed Firewall



- Firewall on Network Interface Card (NIC)
- Hardware based cryptographic accelerator
- Trustworthy control of untrustworthy OS



Made by Secure Computing and 3Com
Research performed under DARPA sponsorship



Hardened Client Timeline



-
- **MARFORPAC Limited Objective Experiment**
 - ◆ Apply safe e-mail wrappers and encrypting file system
 - ◆ MARFORPAC approved internal experiment charter
 - ◆ Execution: Late CY2001, RSO&I 02, UFL 02
 - **Fleet Battle Experiment India (C3F)**
 - ◆ Execution: Jun 2001 – Autonomic Distributed Firewall (PCI)
 - **Fleet Battle Experiment Juliet Goals (PACFLT)**
 - ◆ Complete application of diverse wrappers
 - ◆ Autonomic Distributed Firewall (PCMCIA)



Survivable Server



- **Motivating factors:**

- ◆ High-value and commonly targeted center of gravity
- ◆ Need Intrusion Tolerant Systems:
Ability to confidently execute mission while under attack
- ◆ Reactive defense not adequate

- **Possible technologies:**

- ◆ PASIS: Perpetually Available Survivable Information System
Leverage fragmentation, redundancy, and scattering
- ◆ SELinux, Immunix, Emerald, NetTop Vmware, Wrappers

- **Execution: 2002**



Situational Awareness



-
- **Am I under attack ?**
 - **What is the nature of the attack ?**
 - ◆ Class, mechanism, and source
 - **What is mission impact ?**
 - ◆ Urgency, damage assessment and control, initial response
 - **When did attack start ?**
 - ◆ More detailed damage assessment. What have I done wrong ?
 - **Who is attacking?**
 - ◆ What are they trying to do? What is their next step ?
 - **What can I do about it ?**
 - ◆ Course of action analysis, collateral damage risk, reversibility



Theater C4I Coordination Center PACOM TCCC

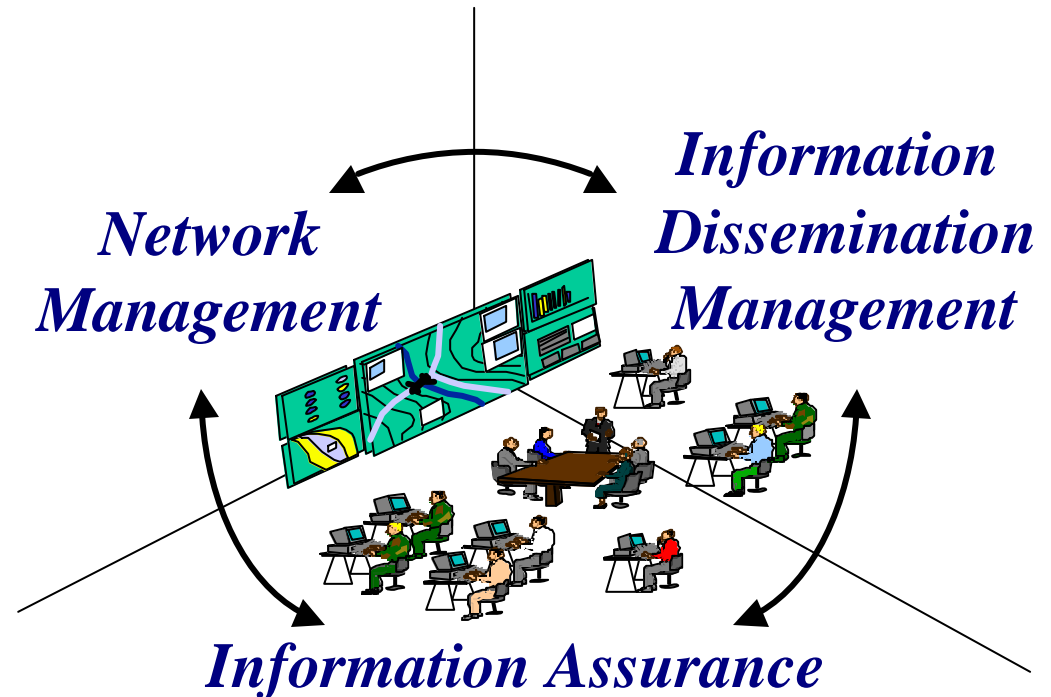
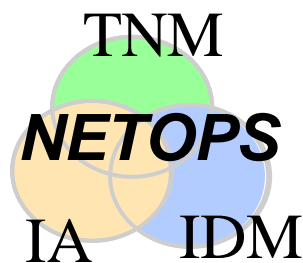


Need

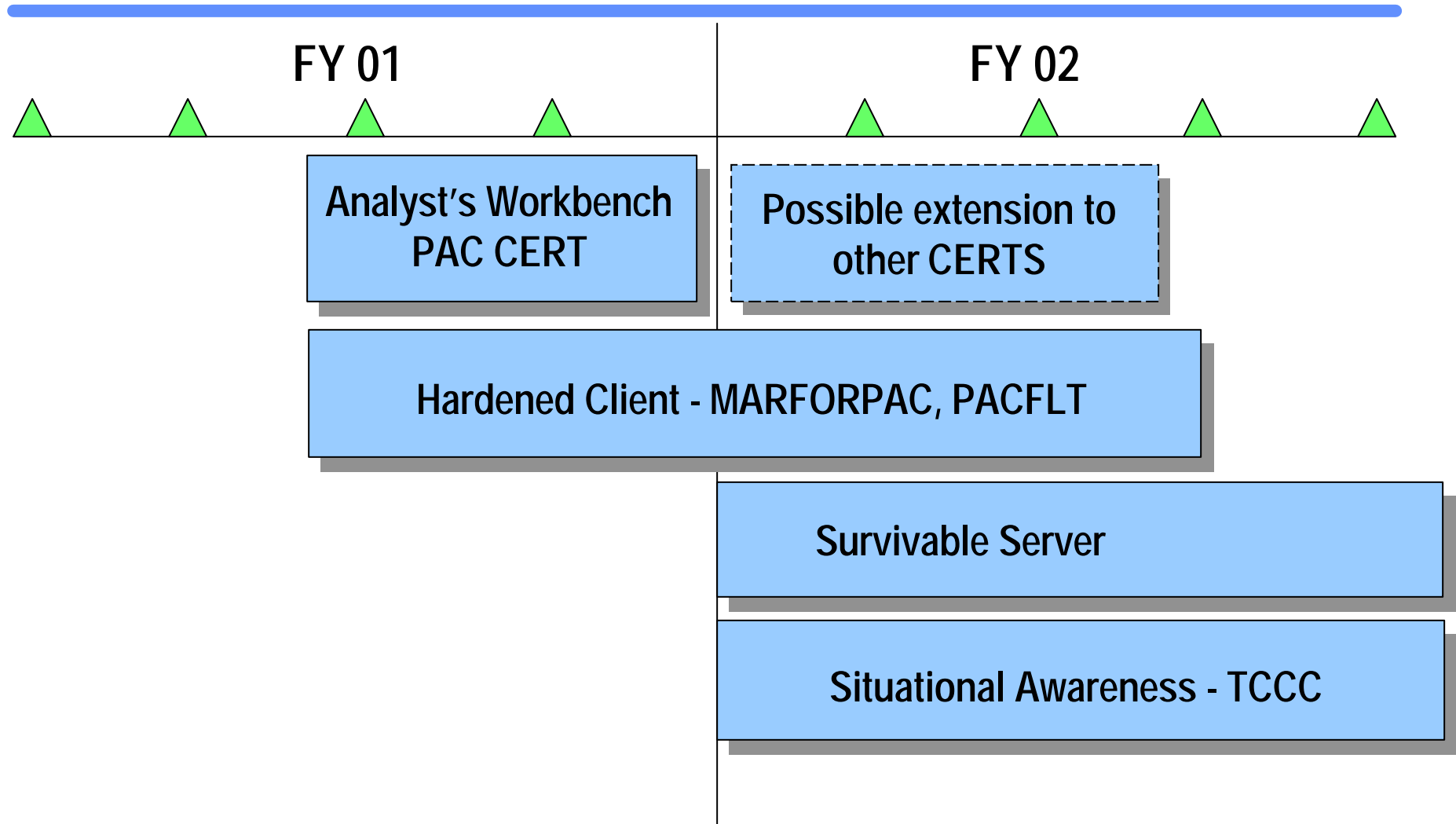
- *Theater Wide*
- *Real Time*
- *Decision Quality*
- *Actionable Information*

Strategy

- Leverage Cyber Panel emerging research

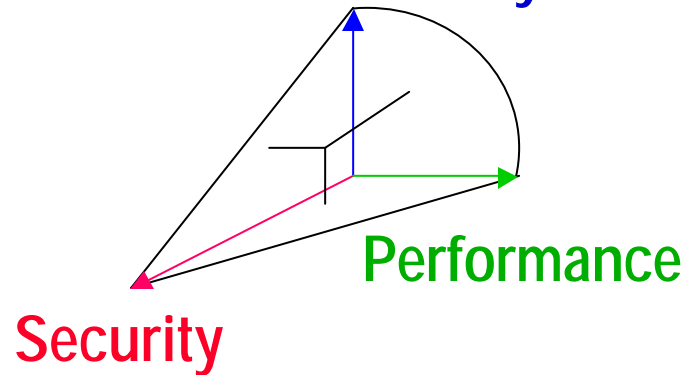


Summary

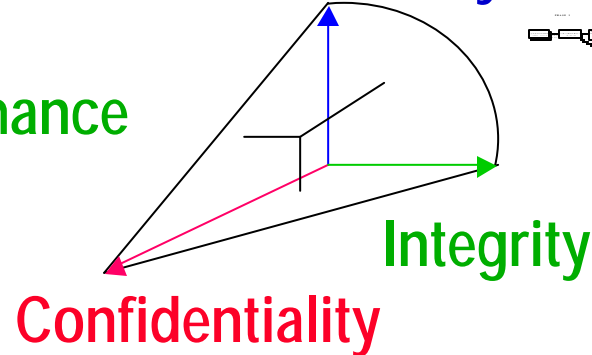




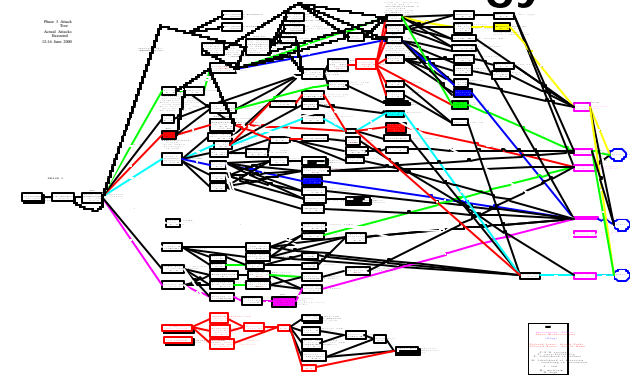
Functionality



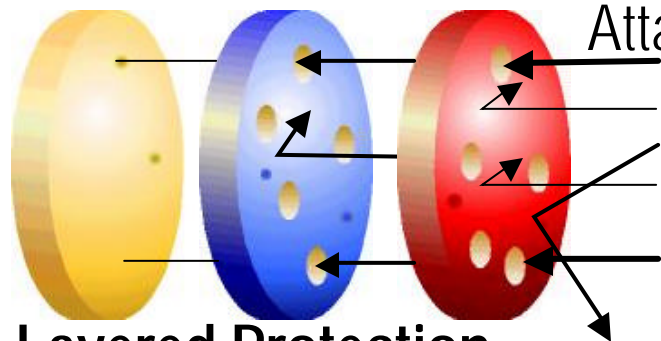
Availability



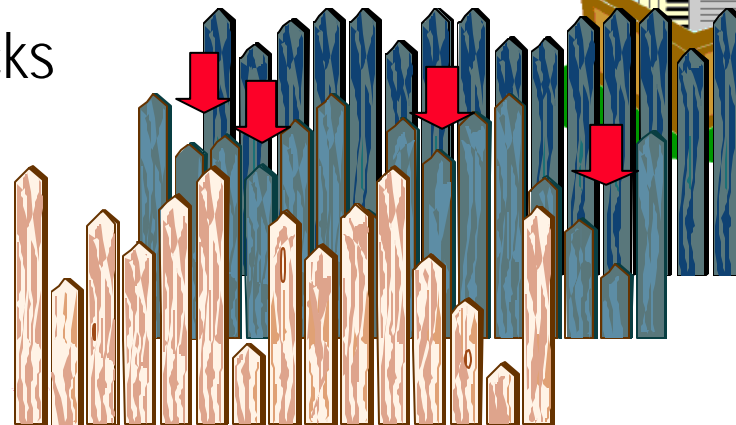
Methodology



Tolerance Detection Prevention



Layered Protection
Dynamic Defense



Risk-Balanced Optimizing Strategy

